

Efficient Oblivious Proofs Of Correct Exponentiation (Make Corrections)
Markus Jakobsson, Claus Peter Schnorr

View or download:
belllabs.com/~markusj/oblivious.ps
belllabs.com/user/markusj/oblivious.ps
Cached: [PS.gz](#) [PS](#) [PDF](#) [DjVu](#) [Image](#) [Update](#) [Help](#)



[Home/Search](#) [Bookmark](#) [Context](#)

[Related](#)

From: belllabs.com/~markusj/ (more)
Homepages: [M.Jakobsson](#) [\[2\]](#) [\[3\]](#) [\[4\]](#) [C.Schnorr](#)
[HPSearch](#) [\(Update Links\)](#)

[\(Enter summary\)](#)

Rate this article: 1 2 3 4 5 (best)

[Comment on this article](#)

Abstract: We study the notion of meta-proofs, which, as the name indicates, are proofs about proofs. We employ the notion of meta-proofs to produce a highly efficient oblivious proof of correct exponentiation. It is minimum knowledge independently of whether the input is valid or not, a property that does not hold for many other protocols (that are zero-knowledge only for valid inputs.) This has direct security implications to multiparty protocols, where the protocols we demonstrate – one interactive and... [\(Update\)](#)

Active bibliography (related documents): [More](#) [All](#)

- 0.3: The Power of RSA Inversion Oracles and the.. - Bellare.. (2001) [\(Correct\)](#)
- 0.3: Security of DL-encryption and signatures against generic attacks.. - Schnorr (2000) [\(Correct\)](#)
- 0.3: Efficient Convertible Undeniable Signature Schemes (Extended .. - Michels, Stadler (1997) [\(Correct\)](#)

Similar documents based on text: [More](#) [All](#)

- 0.1: Flash Mixing - Jakobsson (1999) [\(Correct\)](#)
- 0.1: Security of Signed ElGamal Encryption - Schnorr, Jakobsson (1999) [\(Correct\)](#)
- 0.1: Speeding up Discrete Log and Factoring Based Schemes.. - Boyko, Peinado.. (1998) [\(Correct\)](#)

BibTeX entry: [\(Update\)](#)

```
@misc{ jakobsson-efficient,
  author = "Markus Jakobsson and Claus Peter Schnorr",
  title = "Efficient Oblivious Proofs Of Correct Exponentiation",
  url = "citeseer.nj.nec.com/205854.html" }
```

Citations (may not include all citations):

- 427 How to Share a Secret (context) - Shamir - 1979
- 386 A Public-Key Cryptosystem and a Signature Scheme Based on Di.. (context) - ElGamal
- 321 Random Oracles are Practical: a Paradigms for Designing Effi.. - Bellare, Rogaway - 1993
- 145 Blind Signatures for Untraceable Payments (context) - Chaum
- 91 Security Proofs for Signature Schemes - Pointcheval, Stern - 1996
- 69 How to Share a Function Securely (context) - De Santis, Desmedt et al.
- 57 Undeniable Signatures (context) - Chaum, Van Antwerpen
- 56 Zero-Knowledge Undeniable Signatures (context) - Chaum
- 51 Distributed Provers with Applications to Undeniable Signatur.. (context) - Pedersen
- 35 Efficient Signature Generation for Smart Cards (context) - Schnorr
- 33 Provably Secure Blind Signature Schemes - Pointcheval, Stern - 1996
- 21 Designated Verifier Proofs and Their Applications - Jakobsson, Sako et al.
- 14 Digital Signature Standard (DSS (context) - for, Technology - 1991
- 13 The Random Oracle Methodology, Revisited - Canetti, Goldreich et al. - 1998
- 11 Fast Batch Verification for modular Exponentiation and digit.. (context) - Bellare, Garay et al.
- 6 Interactive Bi-Proof Systems and Undeniable Signature Scheme.. (context) - Fujioka, Okamoto et al.
- 3 Strengthened Security for Blind Signatures (context) - Pointcheval - 1998
- 1 Proving Without Knowing: On Oblivious, Agnostic and Blindfol.. - Jakobsson, Yung

Documents on the same site (<http://www.bell-labs.com/~markusj/>): [More](#)

- Applying Anti-Trust Policies to Increase Trust in a Versatile .. - Jakobsson, Yung (1997) [\(Correct\)](#)
- Reducing Costs in Identification Protocols - Markus Jakobsson (1992) [\(Correct\)](#)
- Proactive Public Key and Signature Systems - Herzberg, Jakobsson, Jarecki.. (1997) [\(Correct\)](#)

[Online articles have much greater impact](#) [More about CiteSeer](#) [Add search form to your site](#) [Submit documents](#) [Feedback](#)

CiteSeer - citeseer.org - [Terms of Service](#) - [Privacy Policy](#) - Copyright © 1997-2002 [NEC Research Institute](#)